REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 U.S.C. § 103 or is directed to non-statutory subject matter under the provisions of 35 U.S.C. § 101. Thus, the Applicants believe that all of these claims are in allowable form.

I. DOUBLE PATENTING

The Examiner submits that claims 1-3 of the present application conflict with claims 7, 8 and 9, respectively, of United States Patent Application No. 09/711,323, filed November 9, 2000 by de Jesus Valdes et al (hereinafter the "'323 Application"). The Applicants respectfully disagree.

Claims 1-3 of the present application explicitly recite the step of updating or assessing (for the purposes of rejecting a match) a minimum similarity requirement for one or more features or a received alert and an existing alert class. Claims 7-9 of the '323 Application do not recite these steps or make mention of a similarity requirement, and are therefore patentably distinct.

Accordingly, the Applicants respectfully request that there is no instance of double patenting in relation to the present Application and the '323 Application.

II. REJECTION OF CLAIMS 1-3 AND 5-6 UNDER 35 U.S.C. § 101

Claims 1-3 and 5-6 stand rejected under 35 U.S.C. § 101 as being allegedly directed to non-statutory subject matter. In response, the Applicants have amended claims 1-3 and 5-6 in order to more clearly recite aspects of the present invention.

Specifically, claims 1-3 and 5-6 have been amended to recite that the respective methods are performed within "an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected". The alerts that are organized in accordance with the recited method are received from the sensors of the intrusion detection system. Thus, the Applicants submit that methods recited in claims 1-3 and 5-6, as amended, are not abstract, but apply, involve, use and advance the technological arts. Accordingly, the Applicants respectfully request that the rejection of claims 1-3 and 5-6 under 35 U.S.C. § 101 be withdrawn.

III. REJECTION OF CLAIMS 1-6 UNDER 35 U.S.C. § 103

1. Claims 1-3 and 5-6

Claims 1-3 and 5-6 stand rejected as being unpatentable over the Kleinman patent (United States Patent No. 6,128,640, issued October 3, 2000, hereinafter "Kleinman"). The Applicants respectfully traverse the rejection.

Particularly, the Applicants submit that the teachings of Kleinman provide no motivation for the adaptation to intrusion detection systems such as that claimed by the Applicants. Kleinman is directed to a method of synchronizing execution of a process with the occurrence of certain events, which is clearly not analogous to a method of providing network security (e.g., in the form of intrusion detection). Moreover, Kleinman is completely devoid of any teaching, allusion or even mention of the need for network security or network intrusion detection. The Applicants therefore respectfully submit that Kleinman is not reasonably pertinent to the problem with which the Applicants are concerned, because a person having ordinary skill in the art of network security would not reasonably have expected to solve the problem of intrusion detection in a computing network by considering a reference dealing with process synchronization. "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992) (MPEP 2141.01(a)). Kleinman is thus clearly a non-analogous reference. The Applicants therefore disagree with the Examiner's conclusion that "it would have been obvious to adapt the teachings of Kleinman in order to obtain greater security and better, more organized response to alerts".

Moreover, even if Kleinman can be considered analogous art, the Examiner's attention is directed to the fact that Kleinman fails to disclose or suggest the novel invention of identifying a set of potentially similar features shared by a new alert and one or more existing alert classes, and then assessing (e.g., updating, setting, or applying) a minimum similarity requirement that must be met or exceeded by one or more features in order to identify a match between a new alert and an existing alert class and/or updating a similarity expectation for one or more of the features, as claimed in Applicants' independent claims 1, 3, 5 and 6.

In contrast, Kleinman, at best, teaches grouping operating system events on which a process can execute (*e.g.*, such that execution of the process is synchronized with the occurrence of one or more of the events). This is <u>not</u> the same as classifying alerts generated by sensors that indicate <u>intrusions or anomalies</u> in a computing system, by <u>updating or setting a minimum similarity requirement</u> for potentially similar features shared by a new alert and one or more existing alert classes. As described in the Applicants' specification (*see*, for example, paragraph 0063 or paragraph 0069), the calculations involved in classifying a sensor alert may be simplified by assigning a minimum similarity value to the features of an alert class. That is, if a feature of a new alert and the corresponding feature of an existing alert class do not match at some minimum similarity value, the new alert cannot be a member of that alert class. Kleinman is completely devoid of any teaching or suggestion relating to the need to update or set <u>a minimum similarity requirement</u> for potentially similar features shared by a new alert and one or more existing alert classes.

Nor does Kleinman teach <u>updating or setting a similarity expectation</u> for certain corresponding features of a new alert and an existing alert class. As described in the Applicants' specification (*see*, for example, paragraphs 0047 - 0061), the nature of an alert may change an expectation of which features of a new alert and an existing alert class should be similar. Both the new alert and the alert class to which it is being compared each compute the similarity expectation for each feature. Feature similarity and similarity expectation are the combined to form a single value of alert similarity. Kleinman is completely devoid of any teaching or suggestion relating to the need to update or set <u>a similarity expectation</u> for certain corresponding features of a new alert and an existing alert class.

The portion of Kleinman that the Examiner cites to support these limitations at best generally describes functions used by objects that represent events on which a process can synchronize. <u>Nowhere</u> in the discussion of these functions, however, is there any mention of the need to update or set a minimum similarity requirement or a similarity expectation relating to a new alert and an existing alert class.

Kleinman thus fails to disclose or suggest the novel invention of <u>assessing (*e.g.*, updating, setting, or applying) a minimum similarity requirement that must be met or exceeded by one or more features in order to identify a match between a new alert and</u>

an existing alert class and/or <u>updating a similarity expectation for one or more of the</u> <u>features</u>, as claimed in Applicants' independent claims 1, 3, 5 and 6. Specifically, Applicants' claims 1, 3, 5 and 6 positively recite:

1.   In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:
    (a) receiving a new alert;
    (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
    (c) <u>updating a minimum similarity requirement for one or more features</u>;
    (d) updating a similarity expectation for one or more features;
    (e) comparing the new alert with one or more alert classes, and either:
    (f1) associating the new alert with the existing alert class that the new alert most closely matches; or
    (f2) defining a new alert class that is associated with the new alert. (Emphasis added)

3.   In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:
    (a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;
    (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;
    (c) comparing the new alert to one or more alert classes;
    (d) rejecting a match <u>if any feature for which a minimum similarity value has been set</u> <u>fails to meet or exceed the minimum similarity value</u>;
    (e) adjusting the comparison by an expectation that certain feature values will or will not match, and either:
    (f1) associating the new alert with the existing alert class that the new alert most closely matches; or
    (f2) defining a new alert class that is associated with the new alert. (Emphasis added)

5. In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:
    (a) receiving a new alert;
    (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;

(c) <u>updating a minimum similarity requirement for one or more features</u>;

(d) comparing the new alert with one or more alert classes, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

6.   In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) comparing the new alert to one or more alert classes;

(d) rejecting a match <u>if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value</u>, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

Accordingly, Kleinman fails to teach, show or suggest every limitation claimed in Applicants' independent claims 1, 3, 5 and 6. Therefore, the Applicants submit that independent claims 1, 3, 5 and 6 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claim 2 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 2 is also not made obvious by the teachings of Kleinman. Therefore, the Applicants submit that dependent claim 2 also fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

2.   Claim 4

Claim 4 stands rejected as being unpatentable over the Kleinman patent in view of the Harrison patent (United States Patent No. 5,517,429, issued May 14, 1996, hereinafter "Harrison"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Harrison, like Kleinman, fails to disclose or suggest the novel invention of <u>assessing (e.g., updating, setting, or</u>

applying) <u>a minimum similarity requirement that must be met or exceeded by one or more features in order to identify a match between a new alert and an existing alert class</u> and/or <u>updating a similarity expectation for one or more of the features</u>, as claimed in Applicants' independent claim 4.

Harrison thus fails to bridge the gap in the teachings of Kleinman. Moreover the Applicants submit that the teachings of the cited references provide <u>no motivation</u> for the combination of Kleinman with Harrison. Specifically, there is no motivation to combine the process execution synchronization method taught by Kleinman with the intelligent area monitoring system taught by Harrison, which monitors or performs surveillance in a physical space. The Applicants therefore disagree with the Examiner's conclusion that it would have been obvious to those of ordinary skill in the art to combine the teachings of Kleinman with those of Harrison and respectfully submit that the Examiner is using hindsight to pick and choose elements from the references to support the rejection.

It is impermissible to use the claims as a framework from which to choose among individual references to recreate the claimed invention. *W. L. Gore Associates, Inc. v. Garlock, Inc.*, 220 U.S.P.Q. 303, 312 (1983). Moreover, the mere fact that a prior art structure could be modified to produce the claimed invention would not have made the modification obvious unless the <u>prior art suggested the desirability of the modification</u>. *In re Fritch*, 23 U.S.P.Q. 2d 1780, 1783, Fed. Cir. (1992); *In re Gordon*, 221 U.S.P.Q. 1125, 1127, Fed. Cir. (1984) (emphasis added). The rules applicable for combining references provide that there must be a suggestion from <u>within the references</u> to make the combination. *Uniroyal v. Rudkin-Wiley*, 5 U.S.P.Q. 2d 1434, 1438 (Fed. Cir. 1988); *In re Fine*, 5 U.S.P.Q. 2d at 1599 (emphasis added). Therefore, the teachings of Kleinman and Harrison do not provide any justification for their combination.

Moreover, incorporating Kleinman's description of process/event synchronization into the systems of Harrison would actually render the systems of Kleinman and Harrison unsatisfactory for their respective intended purposes. The system of Kleinman contemplates the execution of a process is prefaced upon the occurrence of one or more specific events; thus, the process is not executing continuously. In order for a surveillance system such as that taught by Harrison to be effective, it is undesirable for the surveillance system to execute in a manner that is not continuous. That is, if the

system must pause or wait for the occurrence of a given event before running, objects or occurrences that the system is in intended to detect may be missed. Modifying Kleinman such that programs operate continuously, or modifying Harrison to start and stop based on given events, would necessarily change the principle of operation of each modified system. Therefore, the combination of Kleinman and Harrison is inappropriate. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

Finally, the Applicants submit that the Examiner is applying an improper "obvious to try" rationale in support of the rejection of claim 4 over Kleinman in view of Harrison. Specifically, the Applicants submit that Kleinman provides no enabling teachings, guidance or motivation to modify existing area monitoring systems (such as that taught by Harrison). The combination of Kleinman and Harrison fails to provide even general guidance as to the particular form of the Applicants' invention or how to achieve it. *In re O'Farrell*, 853 F.2d 894, 903, 7 USPQ2d 1673, 1681 (Fed. Cir. 1988).

Kleinman in view of Harrison thus fails to disclose or suggest the novel invention of <u>assessing (*e.g.*, updating, setting, or applying) a minimum similarity requirement that must be met or exceeded by one or more features in order to identify a match between a new alert and an existing alert class</u> and/or <u>updating a similarity expectation for one or more of the features</u>, as claimed in Applicants' independent claim 4. Specifically, Applicants' claim 4 positively recites:

4.   In an intrusion detection system that includes a plurality of sensors, each of which generates alerts when attacks or anomalous incidents are detected, a method for organizing the alerts comprising the steps of:
   (a) receiving an alert;
   (b) identifying a set of features that may be shared by the received alert and one or more existing alert classes;
   (c) <u>setting a minimum similarity value for one or more features or feature groups</u>; comparing the new alert to one or more of the alert classes, and either:
   (d1) defining a new alert class that is associated with the received alert if any feature or feature group that has a minimum similarity value fails to meet or exceed its minimum similarity value; or
   (d2) associating the received alert with the existing alert class that the received alert most closely matches. (Emphasis added)

Accordingly, Kleinman in view of Harrison fails to teach, show or suggest every limitation claimed in Applicants' independent claim 4. Therefore, the Applicants submit

that independent claim 4 fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

IV. INFORMATION DISCLOSURE STATEMENT

The Examiner's attention is directed to the fact that the Applicants will be filing a Supplemental Information Disclosure Statement shortly after the filing of this response. Accordingly, it is respectfully requested that the Examiner consider the references listed in the SIDS when considering this response.

V. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §103 and §101. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

_1/9/06_
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702